

JP4115616

Publication Title:

RANDOM CODE GENERATING DEVICE

Abstract:

PURPOSE: To shorten the time required for generating a code by reading in every NS piece of the codes of length (k) generated sequentially from a code converting means, and outputting them after rearranging every NS pieces of the codes in random order by an address generated not from a logical system.

CONSTITUTION: A shift register sequence generator 131 consists of k-pieces of registers and coefficient multipliers and adders less than k-pieces, and generates shift register sequence whose period (n) is longer than NC. The code converting means 123 takes out the required signal sequence from the shift register sequence generator 131, and converts it into the code of the length (k). A code parallel substituting means 133 takes in every NS pieces of the codes of the length (k) generated sequentially from the code converting means 132 in the memory, and rearranges them by every NS pieces in the random order by a means equivalent to the retrieval of a table not by the logical system, and outputs them. But NS is selected so that an integer (m) to satisfy $NS \leq m \times NS \leq n$ exists. Thus, the time required for generating the code can be shortened.

Data supplied from the esp@cenet database - <http://ep.espacenet.com>

⑫ 公開特許公報(A) 平4-115616

⑬ Int. Cl.⁵H 03 K 3/84
H 04 N 7/167

識別記号

Z

庁内整理番号

8221-5J
8943-5C

⑭ 公開 平成4年(1992)4月16日

審査請求 未請求 請求項の数 2 (全19頁)

⑮ 発明の名称 ランダム符号発生装置

⑯ 特 願 平2-231481

⑰ 出 願 平2(1990)8月31日

⑱ 発 明 者 沖 田 茂 神奈川県横浜市磯子区新杉田町8 株式会社東芝横浜事業
所家電技術研究所内

⑲ 出 願 人 株 式 会 社 東 芝 神奈川県川崎市幸区堀川町72番地

⑳ 代 理 人 弁 理 士 伊 藤 進

明 細 書

1. 発明の名称

ランダム符号発生装置

2. 特許請求の範囲

(1) 相異なる長さkの符号をNC個発生するランダム符号発生装置において、

周期nがNCより大なるシフトレジスタ系列を発生するk次のシフトレジスタ系列発生器と、

前記シフトレジスタ系列発生器からの所要の信号系列を取り出し、長さkの符号に変換する符号変換手段と、

前記符号変換手段から逐次的に発生する長さkの符号をNS個ずつメモリに取込み、理論的体系でなく発生したアドレスをもって、NS個分ずつランダムな順序に並べ換えて出力する符号並換手段と

を備えたことを特徴とするランダム符号発生装置。

ただし、 $NC \leq m \times NS \leq n$ を満たす整数mが存在するように、NSを選ぶ。

(2) 上記並換手段は、検索数NSを並べ換えるごとに変化させることを特徴とするランダム符号発生装置。

3. 発明の詳細な説明

〔発明の目的〕

(産業上の利用分野)

本発明は、パケット伝送、データ通信、データ放送、有料放送等に利用できるランダム符号発生装置に関する。

(従来の技術)

高度なセキュリティが要求されるシステムでは、データパケットを伝送する場合に、データパケットに暗号をかけることが多い。

このようなデータパケットDpは、第16図に示すように、有料放送、データ放送等サービスを識別するためのヘッダHdと、受信者を特定するための個別識別番号Idとが、暗号化領域Dsに付加されており、このような構造のデータパケットDpが伝送路を伝送される。これにより、当該データパケットDpは、伝達先の受信者に確実に受信させるこ

とができる。

第17図は、上記データ構造を有するデータパケットが伝送される通信システムを示すブロック図である。

第17図において、個別識別番号Idと、暗号化鍵符号Keyとは、次のように使用される。

送信装置100は、伝送路200を介して受信装置300(0)~300(Nc-1)にデータパケットDpを送出するようになっている。

上記送信装置100は、個別識別番号Idと暗号化鍵符号Keyとを対応させたテーブル101を有している。この送信装置100は、例えば受信装置300(0)にデータパケットを送信する場合、当該テーブル101から個別識別番号Id(0)と暗号化鍵符号Key(0)を取り出し、暗号化鍵符号Key(0)により暗号化回路102において送信情報Ifを暗号化し、第2図に示すように、この暗号化したデータを暗号化領域Dsに配置し、かつ暗号化していない個別識別番号Idを付加して伝送路200に送出する。なお、このテーブル101に個別識別番号Idに対応させた

暗号化鍵符号Keyは、ランダム符号発生装置103から得られる。

受信装置300(0)~300(Nc-1)側では、上述の場合、複号器301(0)は個別識別番号Id(0)が一致するので暗号解読を行うが、その他の複号器301(1)~301(Nc-1)は個別識別番号Id(1)~Id(Nc-1)が不一致であるので暗号解読ができない。暗号解読には、各受信装置300(0)~300(Nc-1)とも、同一の暗号化鍵符号Keyが必要である。この暗号化鍵符号Keyは、複号器301(0)~301(Nc-1)の内部メモリ(図示せず)に個別識別番号Id(0)~Id(Nc-1)とともに書き込まれており、容易には読み出せないようになっている。

ところで、故意に他人の情報を盗用しようとする者に対しては、伝送路200から個別識別番号Idを比較的容易に取り出すことができても、暗号化鍵符号Keyがなければ暗号解読ができないようなシステムとすることにより、他人の情報の盗用を不可能にする安全対策を施している。すなわち、このようなシステムにおいては、個別識別番号Id

は暗号解読のアクションの役割しかしておらず、安全対策上は暗号化鍵符号Keyが重要な役割を持っていることを意味している。

しかしながら、個別識別番号Idに対する暗号化鍵符号Keyの対応づけにおいては、以下の点に留意する必要がある。

(i) 個別識別番号Idと暗号化鍵符号Keyとの関係は、容易に判明する線形結合等で表現されるものであってはならないこと。

このようにする理由は、個別識別番号Idが伝送路200上から比較的容易に取り出すことができるので、個別識別番号Idが判明すれば一定の計算により暗号化鍵符号Keyがわかってしまうからである。これでは、高度なセキュリティは実現できないことになる。

(ii) 個別識別番号Idと暗号化鍵符号Keyは一对一の対応とし、同一の暗号化鍵符号Keyが異なる個別識別番号Idの組とならないこと。

このようにする理由は、故意に、複号器に入力されるパケットモニタの個別識別番号Idをすげか

えることにより、同じ暗号化鍵符号Keyをもつ他人の情報を盗用する可能性を防ぐためである。また、偶然にも伝送路200上で個別識別番号Idの部分がエラーして他人の個別識別番号Idに化け、その化けた個別識別番号Idに対する暗号化鍵符号Keyが自分のものとたまたま同一であって、自分の情報が他人に漏れてしまうことがあり得るからである。

さて、上記(i)項については、ランダムな符号系列を用いることによって実現するのが望ましい。例えば個別識別番号Idを順に並べ、逐次的にランダムな符号系列を発生させ、暗号化鍵符号Keyとして順に対応させてゆく。

また、上記(ii)項の条件を満たすため、過去に発生した符号をメモリに書き込んでおき、発生した符号が過去に発生した符号と重複しないように逐次比較することが必要となる。

第18図は、上述した暗号化鍵符号Keyの発生動作を説明するためのフローチャートであり、このフローチャートはランダム符号発生手段103で

処理される。

第18図において、ランダム符号発生手段103が動作し(ステップ2001)、初期設定($t = 0$, $tc = 0$)がなされる(ステップ2002)。ついで、ランダム符号発生手段103はランダム符号 $C(tc)$ を発生する(ステップ2003)。ついで、定数 j をリセットし、 $j = 0$ とする(ステップ2004)。そして、定数 $j = t$ か否かを判定し(ステップ2005)、定数 $j \neq t$ でなければ符号 $C(tc)$ が暗号化鍵符号 $Key(j)$ であるか否かを判定し(ステップ2006)、 $C(tc) \neq Key(j)$ でなければ j をインクリメント($j = j + 1$)してから(ステップ2007)、再びステップ2005に戻す。

また、定数 $j = t$ か否かを判定し(ステップ2005)、定数 $j = t$ であれば符号 $C(tc)$ を暗号化鍵符号 $Key(j)$ として出力する(ステップ2008)。ついで、 t をインクリメント($t = t + 1$)したのち(ステップ2009)、 t が必要な符号の数 Nc かを判定し(ステップ2010)、 $t \neq Nc$ の場合に tc をインクリメント($tc = tc + 1$)する(ステップ2011)。

なお、ここでとり上げたランダム符号発生の手段103は、詳しくは、理論的体系をもたない符号を発生する手段のことを意味し、例えば、さいころを振って出た目の数字で符号が決まる符号発生手段のことを指す。以下ランダム符号とはこのような発生手段により発生された符号とする。

(発明が解決しようとする課題)

ところで、所要の符号の数 Nc が非常に大きい場合、問題が発生する。例えば上記個別識別番号 Id が30(bit)で構成されている場合、暗号化鍵符号 Key は、 $2^{30} \approx 11$ 億個必要となる。このような場合、(10億+1)番めの暗号化鍵符号 Key を発生させるためには、過去の10億個の符号と重複しないように少なくとも10億回もの比較を行なう必要がある。例えば、1回当たりの比較に要する時間が10(μ S)であるとする、10億回の比較には 10^4 (S)の所要時間がかかり、これは比較するのに2時間半以上時間がかかってしまうという問題がある。

本発明は、上述して問題点に鑑みてなされても

、なお、上記インクリメント(ステップ2011)の場合、ステップ2006で $C(tc) = Key(j)$ のときにも処理される。このインクリメント(ステップ2011)の処理が終了すると、ランダム符号 $C(tc)$ の発生処理に戻る(ステップ2003)。なお、 $t = Nc$ の場合に終了とする(ステップ2012)。

このような処理フローにより、例えば、第6番めの個別識別番号 $Id(5)$ に対応する暗号化鍵符号 $Key(5)$ については、ランダム符号発生手段103が発生した符号 $C(tc)$ (ここで、 $tc \geq 5$ とする)が、過去に発生した暗号化鍵符号 $Key(0) \sim Key(4)$ のすべてと不一致のとき(ステップ2003~2011)、暗号化鍵符号 $Key(5) = C(tc)$ としてメモリに書き込み出力する(ステップ2008~2010、2012)。もし、 $C(tc)$ が $Key(0) \sim Key(4)$ のどれかと一致するならば、次のランダム符号である $C(tc + 1)$ を発生させ、それと $Key(0) \sim Key(4)$ のそれぞれと比較する。これを全部不一致となるまでくり返す。

このようにして、相異なるランダム符号が順次発生される。

のであり、比較の回数を小さくし、かつ符号発生に要する時間を短くすることができるランダム符号発生装置を提供することを目的とする。

(発明の構成)

(課題を解決するための手段)

本発明は、上記目的を達成するため、相異なる長さ k の符号を Nc 個発生するランダム符号発生装置において、周期 n が Nc より大なるシフトレジスタ系列を発生する k 次のシフトレジスタ系列発生器と、前記シフトレジスタ系列発生器からの所要の信号系列を取り出し、長さ k の符号に変換する符号変換手段と、前記符号変換手段から逐次的に発生する長さ k の符号を Ns 個ずつメモリに取込み、理論的体系でなく発生したアドレスをもって、 Ns 個分ずつランダムな順序に並べ換えて出力する符号並換手段とを備えたことを特徴とする。ただし、 $Nc \leq m \times Ns \leq n$ を満たす整数 m が存在するように、 Ns を選ぶ。

また、上記符号並換手段は、検索数 Ns を並べ換えるごとに変化させればよい。

(作用)

上記従来技術においては、 $(t+1)$ 番めの $Key(t)$ の発生に $Id(t)$ を対応させた。一般には、 Id を連番とすると、 $Key(t)$ の引数 t と $Id(t)$ は同一のものになる。 t と $Id(t)$ との関係は、ランダムか否かは問題ではない。 $Key(t)$ と t と関係がランダムで、 t と $Id(t)$ もこれとは独立にランダムならば $Key(t)$ と $Id(t)$ の関係もランダムである。もちろん、 t と $Id(t)$ が線形結合の関係にあっても、 $Key(t)$ と t がランダムならば、 $Key(t)$ と $Id(t)$ もランダムである。したがって、本発明では、次の条件を満たす符号を短時間に発生することである。

第①項

発生順 t と無関係な符号 (ランダム符号 $Rc(t)$) であること。

第②項

所要の符号数を Nc としたとき、 $(t-1) \leq Nc$ で $Rc(t)$ は互いに同一なものが存在しない (重複しない)。

(実施例)

長さ k の符号を Nc 個発生する装置であって、シフトレジスタ系列発生器 131 と、符号変換手段 132 と、符号並換手段 133 とで次のように構成されている。

上記シフトレジスタ系列発生器 131 は、 k 個のレジスタ、1 個以上 k 個以下の係数器、1 個以上 k 個以下の加算器からなり、周期 n が Nc より大なるシフトレジスタ系列を発生する。

上記符号変換手段 132 は、前記シフトレジスタ系列発生器 131 のシフトレジスタの出力、係数器の出力、あるいは加算器の出力から所要の信号系列を取り出して長さ k の符号に変換する。

上記符号並換手段 133 は、前記符号変換手段 132 から逐次的に発生する長さ k の符号を Ns 個ずつメモリーに取込み、理論的体系によらないテーブルの検索に準ずる手段により Ns 個分ずつランダムな順序に並べ換えて出力する。

ただし、 $Nc \leq m \times Ns \leq n$ を満たす整数 m が存在するように、 Ns は選ばれている。

ランダム符号発生装置 13 は、上述したように

以下、図面に基づいて本発明を説明する。

第 1 図は本発明の一実施例を示すブロック図である。

第 1 図において、送信装置 1 は、伝送路 2 を介して受信装置 3 (0) ~ 3 ($Nc-1$) にデータパケット Dp を送出するようになっている。

上記送信装置 1 は、個別識別番号 Id と暗号化鍵符号 Key とを対応させたテーブル 11 を有している。この送信装置 1 は、例えば受信装置 3 (i) (i は任意の整数) にデータパケットを送信する場合、当該テーブル 11 から個別識別番号 $Id(i)$ と暗号化鍵符号 $Key(i)$ を取り出し、暗号化鍵符号 $Key(i)$ により暗号化回路 12 において送信情報 If を暗号化し、この暗号化したデータを暗号化領域 Ds に配置し、かつ暗号化していない個別識別番号 Id を付加して伝送路 2 に送出する。なお、このテーブル 11 に個別識別番号 Id に対応させた暗号化鍵符号 Key は、ランダム符号発生装置 13 から得られる。

ここで、ランダム符号発生装置 13 は、相異なる

構成されている。

第 2 図は、シフトレジスタ系列発生器 131 の一例であって、線形掃還シフトレジスタ回路で構成した例を示すブロック図である。

この線形掃還シフトレジスタ回路で構成したシフトレジスタ系列発生器 131 は、クロック入力端子 CT を設けた k 個のレジスタ $RE10 \sim RE1k-1$ を直列接続してなるレジスタと、係数 ($-h0 \sim -hk-1$) の k 個の係数器 $K10 \sim K1k-1$ と、 $(k+1)$ 個の加算器 $AD11 \sim AD1k$ と、スイッチ SW とからなり、加算器 $AD1k$ に入力端子 $T1$ を接続し、レジスタ $RE11$ の出力に出力端子 $T0$ を接続している。

各レジスタ $RE10 \sim RE1k-1$ の各出力は $a_{t+k-1} \sim a_t$ で示され、係数器 $K1i$ の出力は $(-h_i \cdot a_{t+i})$ で示され、加算器 $AD1i$ の出力は $(-h_i \cdot a_{t+i})$ を $0 \sim i$ まで加算した値を示している。

このようなシフトレジスタ系列発生器 101 において、まず、スイッチ SW を最初に初期値を入

力端子T1より入力するときに開いておき、クロック入端子CTよりクロックをk個入力すると、各レジスタRE10～RE1k-1に初期値がセットされる。その後、入力端子T1の入力信号を“0”とし、スイッチSWを閉じてクロック入端子CTからクロック信号を入力する。これにより、各レジスタRE10～RE1k-1の内容を次々に移すことをくり返すと、出力端子T0からシフトレジスタ系列が出力される。そして、(n-1)クロック目に各レジスタRE10～RE1k-1の内容が元の初期値に戻る。このとき、このk次のシフトレジスタ系列は周期nをもつという。

第3図は、シフトレジスタ系列発生器131の他の例であって、線形シフトレジスタ回路で構成した例を示すブロック図である。

この線形シフトレジスタ回路で構成したシフトレジスタ系列発生器131は、クロック入力端子CTを設けたk個のレジスタRE21～RE2kを直列接続してなるレジスタと、係数(-h0～-hk-1)のk個の係数器K20～K2k-1と、k個の加

算器AD20～AD2k-1と、スイッチSWとからなり、加算器AD20に出力端子T1を接続し、レジスタRE2kの出力に出力端子T0を接続している。なお、スイッチSWは、最初初期値を入力端子T1より入力するときに開いておく。

このような線形シフトレジスタ回路で構成したシフトレジスタ系列発生器131によっても第2図と同様にk次のシフトレジスタ系列を得ることができる。

ところで、上記各シフトレジスタ系列発生器131において、扱う符号が2元シンボル{“0”、“1”}で構成されるならば、これらは2を法とする乗算、加算になる。また、q元シンボル{0, 1, …, q-1}ならば、qを法とする乗算、加算になる。したがって、例えばq=3の場合には、k=3次のシフトレジスタ系列が発生することになる。

第4図は、q=3の場合のシフトレジスタ系列発生器131の実構成例であって、3元M系列符号発生回路を示している。

この3元M系列符号のシフトレジスタ系列発生器131aは、3個のレジスタRE30～RE32を直列接続してなるレジスタと、係数(-h0または-h1)の1個の係数器K30と、2個の加算器AD31～AD32と、スイッチSWとからなり、加算器AD32に出力端子T1を接続している。各レジスタRE30～RE32の出力をQ[0]～Q[2]とする。

この実施例は、シフトレジスタ系列の中でも同一の段数で周期が最大の系列(M系列)を発生する。一般にM系列の周期は、 $n = q^k - 1$ である。このような周期nをもつk次のシフトレジスタ系列発生器からは、適当に符号を取り出すことにより長さkの符号が周期nで得られる。例えば、第4図の実例のように、q=3の場合のk=3次のシフトレジスタ系列発生器131aからは、 $n = (3^3 - 1) = (27 - 1) = 26$ が得られ、一周が26をもつシフトレジスタ系列が発生することになる。

ここで、係数器K30は、 $(-h_0 = (-1 \bmod$

$3) = 2)$ 、または $(-h_1 = (-2 \bmod 3) = 1)$ となる。また、 $\bmod 3$ は、3を法とする演算を意味し、上記シフトレジスタ系列発生器131aは生成多項式 $H(x) = x^3 + 2x + 1$ を満足する。

このようなシフトレジスタ系列発生器131aにより得られたシフトレジスタ系列を第5図に示す。

第5図(a)は、レジスタRE30～RE32に初期値(“0” “1” “0”)をセットしたときに、シフトレジスタ系列発生器131aから得られるシフトレジスタ系列の説明図である。

時間(time)の経過に伴う、各レジスタRE30～RE32の出力Q[2], Q[1], Q[0]の値と、十進法(10)の値とが示されている。

ここで、各レジスタRE30～RE32の出力Q[2], Q[1], Q[0]の値を十進法(10)に変換するためには、

$$10a = 3^2 \times Q[2] + 3 \times Q[1] + Q[0]$$

を使用すればよい。

第5図(b)は、レジスタRE 30～RE 32に初期値("2" "0" "0")をセットした場合に、シフトレジスタ系列発生器131aから得られるシフトレジスタ系列の説明図である。

このような初期値の場合の時間(time)の経過に対する、各レジスタRE 30～RE 32の出力Q[2], Q[1], Q[0]の値と、十進法(dec)の値とが示されている。

この符号系列の特徴は、シフトレジスタ系列の状態が、各レジスタRE 30～RE 32の内部状態の組合せで一意に決まる点である。したがって、この例では、第5図(a)または同図(b)に示すように、初期値のいかんによらず、

$(Q[2], Q[1], Q[0]) = (200)$ の次のタイムスロットでは、必ず $(Q[2], Q[1], Q[0]) = (020)$ となる。

次に、符号変換手段132の構成例を説明することにする。

符号変換手段132の一番簡単な構成は、シフトレジスタ系列発生器131の具体例として第4

図に示した回路における各レジスタRE 30～RE 32の出力をそのまま取り出すようにした回路構成とすればよい。

このような符号変換手段132によれば、逐次的(シーケンシャル)に出力される符号系列の連続したn個は互いに重複することがない(同一のものはない)。

これらの符号系列は、 $n \geq Nc$ とすることにより、上記条件②項を満足することになる。また、この条件②項を満足するために、従来必要だった過去に発生した符号との比較は、本実施例では不要となる。しかしながら、この構成例は、上記の条件①項を満たしてはいない。なぜなら、これらの符号系列は、線形演算により発生されたものだからである。

そこで、上記条件①項を満たすためには、上記符号変換手段132の出力L(t)に対して、符号並換手段133を用いて符号の並べ換えをすればよい。

まず、符号並換手段133は、上記符号変換手

段132の出力L(t)より逐次的に得られるNs個の符号の組L(t), L(t+1), ..., L(t+Ns-1)をメモリに、順に書き込む。次に、符号並換手段133は、理論的体系を持たないメモリアドレスを発生させる手段により、前記データを前記メモリから取り出してランダムに並べ換える。この出力を、R(t), R(t+1), ..., R(t+Ns)とする。このとき、並べ換えるのは、Ns個の符号の範囲内である。したがって、過去に発生した符号と重複しないように比較する符号の対象は、(t+Ns-1)番めの符号発生するとき最大であって、(Ns-1)個である。すなわち、1億番目の符号発生においても、10億番目の符号発生においても、比較する符号の対象は(Ns-1)個以下となる。

第6図は、上記構成の動作を説明するために示すフローチャートである。

まず、送信装置1において動作が開始する(ステップ601)。ついで、送信装置1がリセットされ、ランダム符号発生装置13もリセット(t=

0, tc=0)されることになる(ステップ601)。ついで、ランダム符号発生装置13のシフトレジスタ系列発生器131は、シフトレジスタ系列を発生する(ステップ602)。ついで、例えば第4図のシフトレジスタ系列発生器131aの各レジスタの出力から直接取り出すことにより構成された符号変換手段132をもって、長さkの符号への変換を行い、出力L(t), L(t+1), ..., L(t+Ns-1)を得る(ステップ604)。

ついで、符号並換手段133は、上記符号変換手段132の出力L(t)より逐次的に得られるNs個の符号の組L(t), L(t+1), ..., L(t+Ns-1)をメモリに、順に書き込む(ステップ605)。これは、以下のようにする。

符号並換手段133のメモリの

0番地のアドレスにL(t)を、

1番地のアドレスにL(t+1)を、

...

i番地のアドレスにL(t+i)を、

...

($Ns - 1$)番地のアドレスに $L(t + Ns - 1)$ をそれぞれ書き込む。

次に、 $i = 0$ とする(ステップ606)。そして、理論的体系を持たないメモリアドレスを発生させる手段により、ランダムアドレス $C(t)$ を発生させる(ステップ607)。ただし、ランダムアドレス $C(t)$ は、 $0 \leq C(t) \leq (Ns - 1)$ の関係が成立するものとする。

ついで、定数 j をリセットし、 $j = 0$ とする(ステップ608)。そして、定数 $j = i$ か否かを判定し(ステップ609)、定数 $j = i$ でなければ $L(t + C(t)) = R(t + j)$ であるか否かを判定し(ステップ610)、 $L(t + C(t)) = R(t + j)$ でなければ j をインクリメント($j = j + 1$)してから(ステップ611)、再び定数 $j = i$ か否かの判定(ステップ609)に戻る。

また、定数 $j = t$ か否かを判定し(ステップ609)、定数 $j = t$ であれば $R(t + j)$ を $L(t + C(t))$ として出力する(ステップ612)。ついで、 i をインクリメント($i = i + 1$)したのち(ステ

ップ613)、 i が異なる符号の数 Nc かを判定し(ステップ614)、 $i \neq Nc$ の場合に tc をインクリメント($tc = tc + 1$)する(ステップ615)。なお、上記 tc のインクリメント(ステップ615)の処理は、 $L(t + C(t)) = R(t + j)$ と判定されたときにも(ステップ610)、実行される。このインクリメント(ステップ615)の処理が終了すると、ランダムアドレス $C(tc)$ の発生処理に戻る(ステップ607)。

なお、 $i = Nc$ の場合(ステップ614)、 $t = t + Ns$ の処理をし(ステップ616)、ついで、 $(t \leq Nc - 1)$ であるなら(ステップ617)、シフトレジスタ系列の発生処理(ステップ602)に戻る。また、 $(t > Nc - 1)$ であるなら(ステップ617)、全ての処理を終了する(ステップ618)。

このように動作することにより、シフトレジスタ系列発生器131からシフトレジスタ系列が発生し、このシフトレジスタ系列を符号変換手段132で符号変換し、その符号変換した出力を符号

並換手段133でランダムに並べ換えることにより、ランダム符号が発生することになる。

このように本実施例で発生するランダム符号は、従来のものと比べて短時間で得ることができることになる。これを以下に説明する。

従来の方法では、第18図のフローチャートに示すように t 番めの出力は、比較の対象が $(t - 1)$ 個存在した。これと同様なフローで Ns 個の符号をランダムな順序に出力するとすれば、 $R(t + i)$ 、[ただし、 $0 \leq i \leq (Ns - 1)$ である]の発生においては、 $(i - 1)$ 個が比較の対象となる。第6図に示すフローチャートにおいて、ステップ605以降のステップが符号並換手段133で処理される。

上記メモリアドレス $C(t)$ の発生確率を一概(それぞれ $1/Ns$)とすると、 $R(t + Ns - 1)$ を発生するのに必要なメモリの読み出し回数は、平均 Ns 回である。このうち、 $(Ns - 1)$ 回は、 $(Ns - 2)$ 個の符号 $R(t)$ 、 $R(t + 1)$ 、 \dots 、 $R(t + Ns - 2)$ のいずれかと一致する。このとき読み出

した符号について、この順に比較するとすれば、それぞれと一致する確率は等しく、 $1/Ns$ である。また、一致検出までの比較(第6図のステップ607~609による)の回数は、それぞれ、1、2、 \dots 、 $(Ns - 1)$ であるから、この場合の平均比較回数は

$$\{1/(Ns - 1)\} \times \{1 + 2 + (Ns - 1)\} \\ = Ns / Ns - 1 \quad \dots (1)$$

である。

最後の Ns 回目は、必ず $(Ns - 1)$ 回の比較を行うので、 $R(t + Ns - 1)$ を発生するのに比較する平均回数 $Ncmp$ は、

$$Ncmp = (Ns - 1) \times \{Ns / (Ns - 1)\} \\ + (Ns - 1) = 2Ns - 1 \quad \dots (2)$$

である。

$R(t + i)$ 、ただし、 $0 \leq i < (Ns - 1)$ を発生するときの比較対象は、 $(i - 1)$ 個の符号なので、平均比較回数は、上記(2)式の $Ncmp$ より小である。

例えば、 $Ns = 100$ としたとき、上記(2)式

より平均比較回数は、せいぜい199程度であり、従来では(10億+1)番目の符号出力に対して、10億回以上の比較を必要としていた方法に比べ格段に発生時間を短縮できる。

上述の実施例の場合を従来のもものと比較してみると、 $199/10^9 \approx 2/10^7$ 以下に短縮することができることを意味している。

なお、Ns を毎回固定とすると、シフトレジスタ系列の周期 n に関して、

$$Nc \leq m \times Ns \leq n \quad \dots (3)$$

なる整数 m が存在するという条件が必要である(実施例参照)。

また、並べかえの個数 Ns を可変とすることも可能であり、このとき i 番めの並べ換えを Ns i とすると、上記第(3)式は、

$$Nc \leq \sum_{i=1}^n Ns i \leq n \quad \dots (4)$$

という整数 m が存在するという条件におき変わることになる。

一般に、Nc と n が近い数のとき、最後の m 番めの並べ換えにて、第(4)式を満たすように、

Ns を小さく選べばいい。例えば、Nc = 250 であって、n = 255 のとき、

$$Ns1 = Ns2 = Ns3 = 80 \text{ であるとする。}$$

$$250 - 80 \times 3 \leq Nsm = Ns4 \leq 255 - 80 \times 3$$

$$10 \leq Ns4 \leq 15 \quad \dots (5)$$

とすれば、上記第(4)式は満たされることになる。

また、Ns を毎回ランダムに変化させると、R(t) のランダム性も大となる。

なお、長さ k の符号への符号変換手段 132 は、ハードウェアイメージで、N 個の符号並換手段 133 はソフトウェアイメージで説明してきたが、相方ともソフトでもハードでも実現できる。例えば、k 次シフトレジスタ系列の発生は、レジスタの内容をまわるようにプログラムを組めば発生できる。

本発明の一実施例は、上記したようになっている。

次に、本発明の他の実施例を以下に説明する。

第7図は、長さ k = 8 のシフトレジスタ系列発

生器の構成例を示すブロック図である。

第7図に示す8次のシフトレジスタ系列発生回路 811 は、第2図に示す線形帰還シフトレジスタ回路の変形例である。

この図では、レジスタ 800 ~ 807 と、加算器 808 ~ 810 とで、8次のシフトレジスタ系列発生回路 811 が構成されている。このシフトレジスタ系列発生回路 811 は、第2図の構成とは異なって初期値を入力するための入力端子 TI と、スイッチ SW と、シフトさせるためのクロック入力端子 CT とを省略している。このシフトレジスタ系列発生回路 811 の信号のうち、Q[7], Q[6], Q[5], Q[4], Q[3], Q[2], Q[1], Q[0] を選ぶことにより、長さ k の符号を得られる。

このとき、長さ 8 の符号への符号変換手段 812 は有形無形であるが、一般には第8図に示される論理回路で構成できる。

第8図において、論理回路 812a は、Q[7], Q[6], Q[5], Q[4], Q[3], Q[2], Q[1], Q[0], Q'[4], Q'[3], Q'[2] の入力端子と、L(t) = (b

7, b6, b5, b4, b3, b2, b1, b0) の出力端子と、およびセレクト信号入力端子とを設けている。

ただし、信号の組合せ方にはある制限がある。前にも説明したように、シフトレジスタ系列発生器の状態は、シフトレジスタ 811 の内容で一意に決定される。発生された符号 L(t) が、周期 n をもつためには、L(t) と各レジスタの内容の組合せが一对一対応とならなければならない。したがって、Q[4] と、Q'[4] とを同時に選ぶと、レジスタ 804 の内容が重複するので、他のレジスタのうちどれかひとつは抜けることとなる。

一般には、第2図で示す型式のシフトレジスタ発生回路を用いた場合、右から i 番めのレジスタに関しては、 a_{t+i} 、 $-h_i \cdot a_{t+i}$ 、 $\Sigma(-h_i \cdot a_{t+i})$ のうち少なくともどれかひとつを符号 L(t) の要点として選ぶことが、L(t) が周期 n をもつことの必要十分条件である。また、当然のことながら、第8図において L(t) の発生途中でセレクト信号を変化させ、組合せを変えると周

期 n は保証されない。

第7図のシフトレジスタ系列発生回路811を用いた生成多項式 $H(x)$ は、

$$H(x) = x^8 + x^4 + x^3 + x^2 + 1$$

の場合の長さ8の符号 $L(t)$ の発生例を次に説明することにする。

第9図(1)～同図(3)は、初期値を $(Q[7], Q[6], Q[5], Q[4], Q[3], Q[2], Q[1], Q[0]) = (10101011)$ とすると、時刻(time)に対する、出力 $Q[7], Q[6], Q[5], Q[4], Q[3], Q[2], Q[1], Q[0]$ の値と、出力 $Q'[4], Q'[3], Q'[2]$ の値と、十六進数 ma, mb, mc の値を示している。

また、十六進数 ma, mb, mc は、長さ8への変換の例として、

$$ma = (Q[7], Q[6], Q[5], Q[4], Q[3], Q[2], Q[1], Q[0])$$

$$mb = (Q[7], Q[6], Q[5], Q'[4], Q'[3], Q'[2], Q[1], Q[0])$$

$$mc = (Q[7], Q[6], Q[5], Q'[4], Q'[3],$$

タ系列発生器の実施例を示す。

M系列でない8次のシフトレジスタ系列発生器811bは、第7図のシフトレジスタ系列発生器811とは、加算器808a, 809a, 810a, 810bで、出力 $Q[7], Q[6], Q[4], Q[1]$ を加算して、レジスタ807に入力し、 $Q'[7], Q'[6], Q'[4], Q'[1]$ を得られるようにした点が異なる。

このシフトレジスタ系列発生器811bによれば、生成多項式 $H(x)$ は、

$$H(x) = (x+1)^3 (x^3 + x^2 + 1) \\ = x^8 + x^7 + x^6 + x^4 + x + 1$$

として得られる。

これは、初期値を $Q[7] \sim Q[0]$ の順に、 (10000000) のようにセットすると、

$$n = 4 \times 31 = 124 \quad \dots (6)$$

の周期をもつ系列を発生する。

この系列を、長さ8の符号の符号変換手段により以下のように変換する。

第12図(1)、同図(2)は、初期値が $(Q[7] \sim Q[0]) = (10000000)$ のときに、

$$Q'[2], Q[1], Q[0])$$

で求められる。

第10図は長さ8の符号への符号変換手段を、シリアル/パラレル変換回路を用いて構成した例を示すブロック図である。

長さ8の符号への符号変換手段812bは、レジスタ $RE80 \sim RE87$ を直列接続し、各レジスタ $RE80 \sim RE87$ にクロックを入力可能し、レジスタ $RE88$ に出力 $Q[0]$ を入力し、かつ各レジスタ $RE80 \sim RE88$ の出力から出力 $L(t) = (b7, b6, b5, b4, b3, b2, b1, b0)$ を得るようしたものである。

このクロック信号は、第7図に示すシフトレジスタ系列発生回路811のシフトクロックと同一のものである。この場合、 $L(t)$ は8クロック前の第7図のシフトレジスタ系列発生回路811の各レジスタの内容と一致する。

シフトレジスタ系列は、M系列だけとは限らない。

第11図に、M系列でない8次のシフトレジス

一周期 $n = 124$ における時刻(time)に対する、出力 $Q[7] \sim Q[0]$ の値と、出力 $Q'[7], Q'[6], Q'[4], Q'[1]$ の値と、三つの十六進数 ma, mb, mc の値(符号変換手段の値)をそれぞれ示されている。

また、十六進数 ma, mb, mc は、長さ8への変換の例として、

$$ma = (Q[7], Q[6], Q[5], Q[4], Q[3], Q[2], Q[1], Q[0])$$

$$mb = (Q'[7], Q'[6], Q[5], Q'[4], Q[3], Q[2], Q'[1], Q[0])$$

$$mc = (Q'[7], Q[6], Q[5], Q'[4], Q[3], Q[2], Q'[1], Q[0])$$

で求められる。

第13図は、初期値が $(Q[7] \sim Q[0]) = (11010000)$ のときに、一周期 $n = 64$ における時刻(time)に対する、出力 $Q[7] \sim Q[0]$ の値と、出力 $Q'[7], Q'[6], Q'[4], Q'[1]$ の値と、三つの十六進数 ma, mb, mc の値(符号変換手段の値)をそれぞれ示されている。

また、十六進数 m_a, m_b, m_c は、長さ8への変換の例として、

$$m_a = (Q[7], Q[6], Q[5], Q[4], Q[3], Q[2], Q[1], Q[0])$$

$$m_b = (Q'[7], Q'[6], Q[5], Q'[4], Q[3], Q[2], Q'[1], Q[0])$$

$$m_c = (Q'[7], Q[6], Q[5], Q'[4], Q[3], Q[2], Q'[1], Q[0])$$

で求められる。

上記は、同じ回路で初期値のみを変えたものである。簡便には、第15図と16図で取り得ないレジスタの値を初期値として与えてみると、 $n = 124$ の場合と、 $n = 62$ の場合とで、 S_a 同士で比較すると、一致する符号がないことがわかる。これは、シフトレジスタ系列発生器の状態がレジスタの内容に代表されるからで、124種のAグループと、62種のBグループとが存在し、それぞれグループ内のどの初期値を読み込んでも周期 $n = 124$ か、 $n = 62$ の符号 $L(t)$ を発生することができる。また、初期値の操作により、 $L(t)$ として

る。

$L(t)$ の符号は並べ換え前で、第9図(1)の m_a と同一である。 $R(t)$ は、並べ換え後で最初の90個を示す。 N_s 個内での比較は、符号自体で行ったが、過去に発生したメモリアドレスとの比較でも可能である。 $L(t)$ の N_s 個をランダムに並べ換えることは、 $0 \sim (N_s - 1)$ のアドレスをランダムに、しかも重複しないで発生することに等価である。

したがって、たとえばアドレスを $(7, 0, 11, 10)$ と過去に発生したならば、次に発生するアドレスは $(7, 0, 11, 10)$ 以外であればよい。

このために、第6図のフローチャートにおいて、ステップ610での比較は、アドレスであるもの同士を比較すればよい(つまり、 $C(t) = i$ かとする)。この場合、 $N_s = 30$ ならば、 j は $0 \leq j \leq 29$ なので、5ビットで表現でき、その比較は5ビットでよいことになる。もしも、 $R(t)$ として、50ビット必要ならば、比較のビット数は、1/10に

AグループとBグループに対応する符号が混在するものも得ることができる。例えば、初期値 (10000000) より順次符号 $L(t)$ を発生させ、途中で時間(time) ($t = 50$) において、強制的に (11010000) を読み込ませるとAグループからBグループに移る。

そして、 $L(50)$ から $L(50 + 61)$ を発生したとこれで、再び初期値を、第12図(1)の時間(time) ($t = 50$) に対応するところの (10010011) を読み込ませると、再びAグループにもどる。このように、 $n = 124 + 62 = 186$ 個の重複しない符号 $L(t)$ を得ることができるわけである。

シフトレジスタ系列の特徴は、こうしたことが第12図、第13図をあらかじめ持っていなくても逐次的な操作で可能であることが大きな特徴であり、 n が大の場合に有効である。

次に、 N_s の符号の符号並換手段の実施例を第14図に示す。

並べ換えの動作は、第6図に示すフローチャートにより行うものとし、 $N_s = 30$ の場合の例であ

なる。

また、メモリアドレスの発生順序を、 N_s 個の並べ換えごとに変えることは必ずしも必要でなく、テーブルとして固定のランダムなアドレスのセットを持っていたもよい。この場合は、第6図のフローチャートのステップ601は、「 $t \leftarrow 0$ 、 $t_c \leftarrow 0$ 」について、「 $t \leftarrow 0$ 」とし、同図フローチャートのステップ608の「 $j \leftarrow 0$ 」を「 $j \leftarrow 0$ 、 $t_c \leftarrow 0$ 」とすることに相当する。

第15図は、第14図の $L(t)$ 、 $R(t)$ のものと同じ系列であり、 $N_c \leq m \times N_s \leq n (\dots (3))$ 式を満たさないものの例である。

すなわち、上記例は、上記第(3)式を満たさないときは、この例のように、 $R(242) = (29)_{\text{hex}} = (00101001) = R(10)$ において重複することになる。

このような実施例によっても、符号並換手段が実現することができる。

本発明の実施例は、上述したように、必要なランダム符号 $R(t)$ の数 N_c が大きいとき、符号発

生に要する時間の短縮する効果がある。また、本実施例では、 $R(t)$ の符号発生時に要する時間の比率は、並べ換えの個数 N_s に対し、 $\{(2N_s - 1)/t\}$ 以下であり、 $t = 10^9$ 、 $N_s = 10^0$ とすれば、 $2/10^9$ 以下の時間で発生できることになる。

〔発明の効果〕

以上説明してきたとおり、本発明は、必要なランダム符号 $R(t)$ の数 N_c が大きいとき、符号発生に要する時間の短縮できる効果がある。また、本発明は、 $R(t)$ の符号発生時に要する時間の比率は並べ換えの個数に対して著しく短い時間で発生することができる。

4. 図面の簡単な説明

第1図は本発明の一実施例の全体構成を示すブロック図、第2図は同実施例の線形掃型形のシフトレジスタ系列発生器を示すブロック図、第3図は同実施例の線形形のシフトレジスタ系列発生器を示すブロック図、第4図は同実施例の3元M系列のシフトレジスタ系列発生器の具体例を示すブ

ロック図、第5図は第4図の発生器で得られる符号の発生例を示す説明図、第6図は同実施例の動作を説明するために示すフローチャート、第7図は同実施例のシフトレジスタ系列発生器および符号変換手段の具体例を示すブロック図、第8図は同実施例の符号変換手段の例を示すブロック図、第9図(1)～(3)は同シフトレジスタ系列の発生例と符号変換例を示す説明図、第10図は同符号変換手段の他の具体例を示すブロック図、第11図は同符号変換手段のさらに他の具体例を示すブロック図、第12図(1)、(2)は同シフトレジスタ系列の発生例と符号変換例を示す説明図、第13図は他のシフトレジスタ系列の発生例と符号変換例を示す説明図、第14図はランダム符号発生 $R(t)$ の発生例を示す説明図、第15図はの変換例を示す説明図、第16図はデータパケットの基本的構成例を説明するための図、第17図は従来例のブロック図、第18図は同従来例の動作を説明するためのフローチャートである。

1…送信装置、2…伝送路、

3(0)～3($N_c - 1$)…受信装置、

12…暗号化回路、

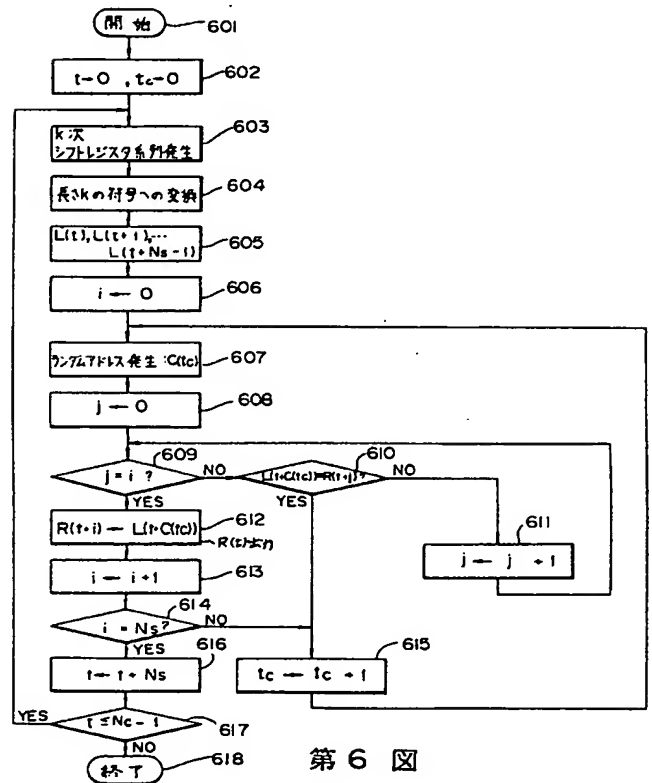
13…ランダム符号発生装置、

131…シフトレジスタ系列発生器、

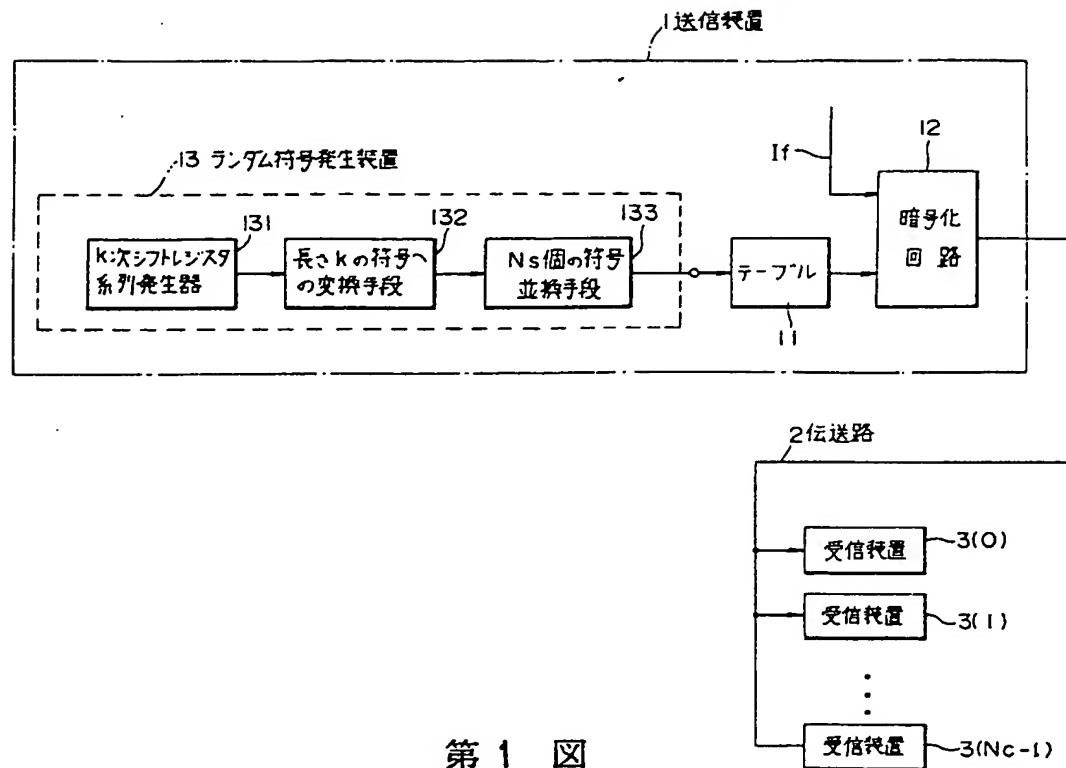
132…符号変換手段、133…符号並換手段。

代理人 井理士 伊 藤 進

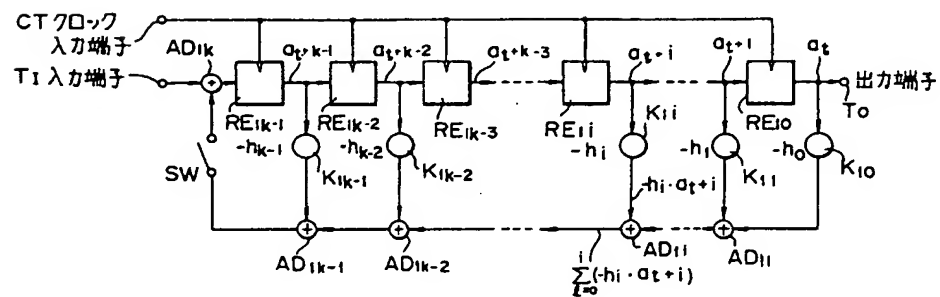
進



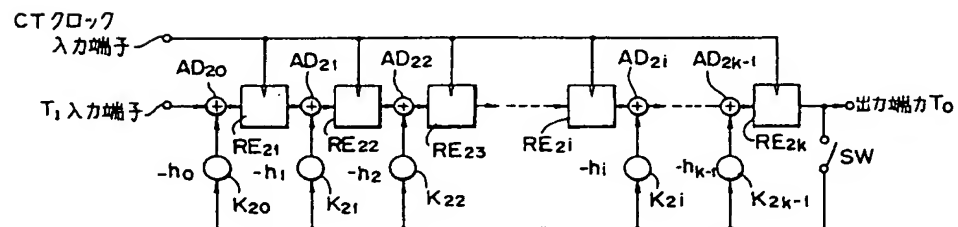
第6図



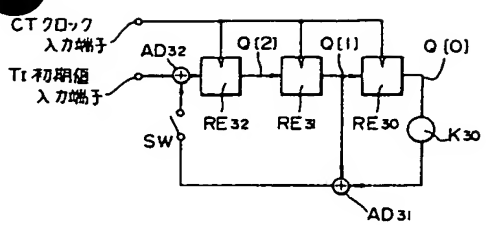
第 1 図



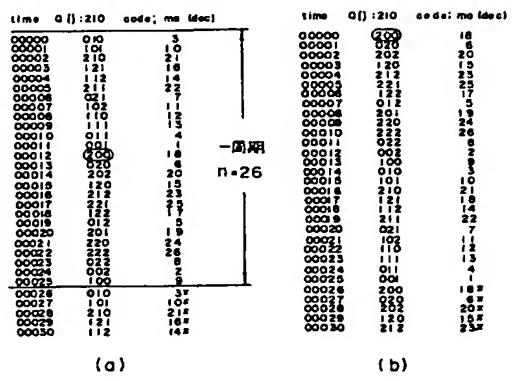
第 2 図



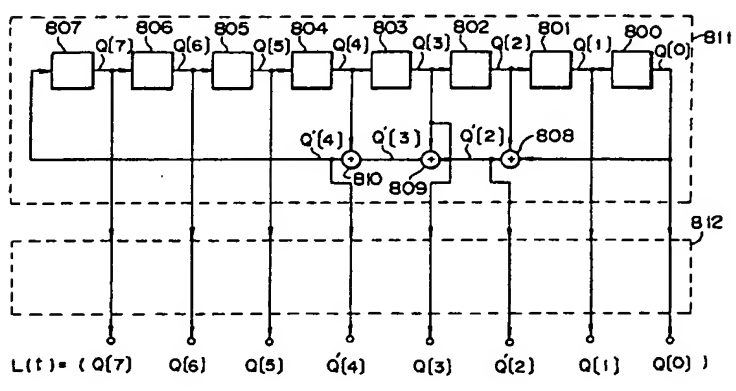
第 3 図



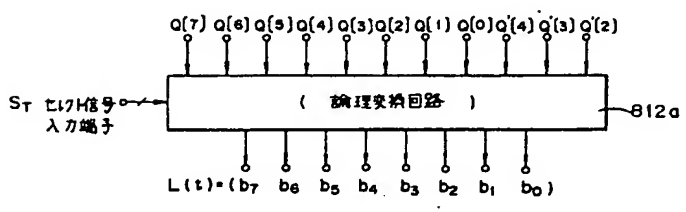
第 4 図



第 5 図



第 7 図



第 8 図

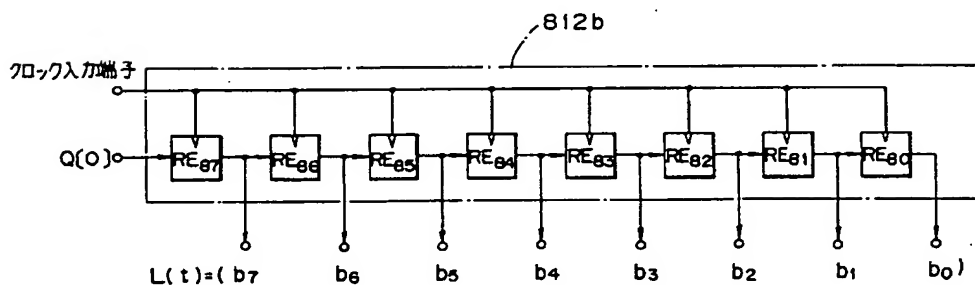
第六圖 (一)

無 9 図 (2)

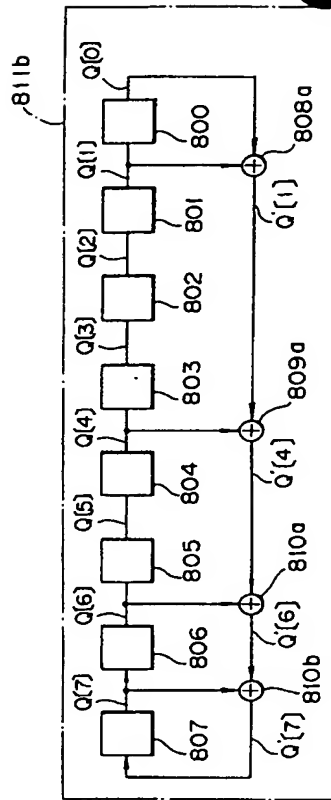
time	Q[1]:78543210	Q'[1]:432	code:	ms	mb	mo	(base)
00198	01010100	011		54	4C	44	
00199	00101010	110		2A	3A	3A	
00200	10010101	100		25	11	11	
00201	11001010	000		0C	01	01	
00202	11001010	000		E5	E1	E1	
00203	01110010	100		72	72	72	
00204	10110010	101		89	85	8D	
00205	11011000	101		0C	04	0C	
00206	11101111	000		77	73	7F	
00207	01110111	101		88	87	BF	
00208	10111011	101		DD	C9	C9	
00209	01101110	001		6E	66	6E	
00210	01101110	001		37	33	33	
00211	00110111	100		9D	99	99	
00212	10011011	101		0D	09	09	
00213	11001010	111		E6	FE	F6	
00214	11100110	111		F3	EF	E7	
00215	01111001	101		79	75	7D	
00216	10111001	101		0C	04	0C	
00217	10111000	101		8C	84	8C	
00218	11011110	101		FE	F6	F6	
00219	11011110	101		FE	F6	F6	
00220	11110111	100		F7	F3	F3	
00221	11110111	101		F8	F7	FF	
00222	11111101	010		FD	E9	E9	
00223	01111110	101		7E	76	7E	
00224	10111111	010		4B	4B	4B	
00225	01011111	010		5F	4B	4B	
00226	00101111	110		2F	3B	3B	
00227	10010111	100		97	93	93	
00228	11001011	001		C8	C7	CF	
00229	01001011	000		65	61	61	
00230	01001011	000		65	61	61	
00231	00110100	100		39	35	3D	
00232	11001000	100		CC	C4	CC	
00233	11001100	111		66	7E	76	
00234	10110011	011		83	AF	A7	
00235	01011001	001		32	32	3D	
00236	01011001	001		32	32	3D	
00237	01011001	001		32	32	3D	
00238	00101011	001		28	27	2F	
00239	00101011	001		15	11	11	
00240	10001010	100		8A	9A	9A	
00241	11001010	000		52	C1	C1	
00242	01100010	010		31	2D	25	
00243	00110001	011		18	08	08	
00244	00011000	001		DC	04	0C	
00245	00001100	111		05	1E	16	
00246	10000011	111		01	0D	05	
00247	11000000	000		E0	E0	E0	
00248	01100000	100		70	70	70	
00249	10110000	010		88	A0	A0	
00250	01011000	101		5C	54	5C	
00251	01011000	101		5C	54	5C	
00252	01011000	101		5C	54	5C	
00253	01011000	101		5C	54	5C	
00254	01011000	101		5C	54	5C	
00255	01011000	101		5C	54	5C	
00256	01010101	100		55	51	51	
00257	10101010	110		AA	BA	BA	
00258	11010101	100		0A	D4	D4	
00259	11101010	100		0A	D4	D4	
00260	11101010	100		0A	D4	D4	

一周期
n=255(2⁸-1)

第9図(3)



第10図



第11図

time	Q[]:78543210	Q'[]:7641	code: sa	sb	sc (hex)
00099	01000011	1100	43	C1	C1
00100	10100001	0111	A1	73	23
00101	01010000	0010	50	10	50
00102	00101000	0000	28	28	28
00103	00010100	1110	14	D4	94
00104	10001010	0111	8A	5A	0A
00105	01000101	0011	45	17	47
00106	00100010	1111	22	F2	A2
00107	10010001	1001	91	63	93
00108	11001000	0100	C8	48	48
00109	01100100	1100	64	E4	E4
00110	10110010	1001	82	A2	62
00111	11011001	0101	D9	48	58
00112	01101100	1100	6C	EC	EC
00113	10110110	1001	86	A6	86
00114	11011011	1010	06	99	06
00115	11101101	1011	ED	BF	EF
00116	11110110	0101	F6	66	76
00117	01111011	0010	7B	29	79
00118	00111101	0001	3D	2F	3F
00119	00011110	0001	1E	0E	1E
00120	00001111	0000	0F	0D	0D
00121	00000111	0000	07	05	05
00122	00000011	0000	03	01	01
00123	00000001	1111	01	D3	83
00124	10000000	1000	80*	80*	80*
00125	11000000	0100	C0*	40*	40*
00126	01100000	1100	60*	E0*	E0*
00127	10100000	0110	80*	70*	30*
00128	01010000	0010	50*	18*	58*
00129	00101000	0000	20*	20*	20*
00130	00010100	0001	10*	06*	16*

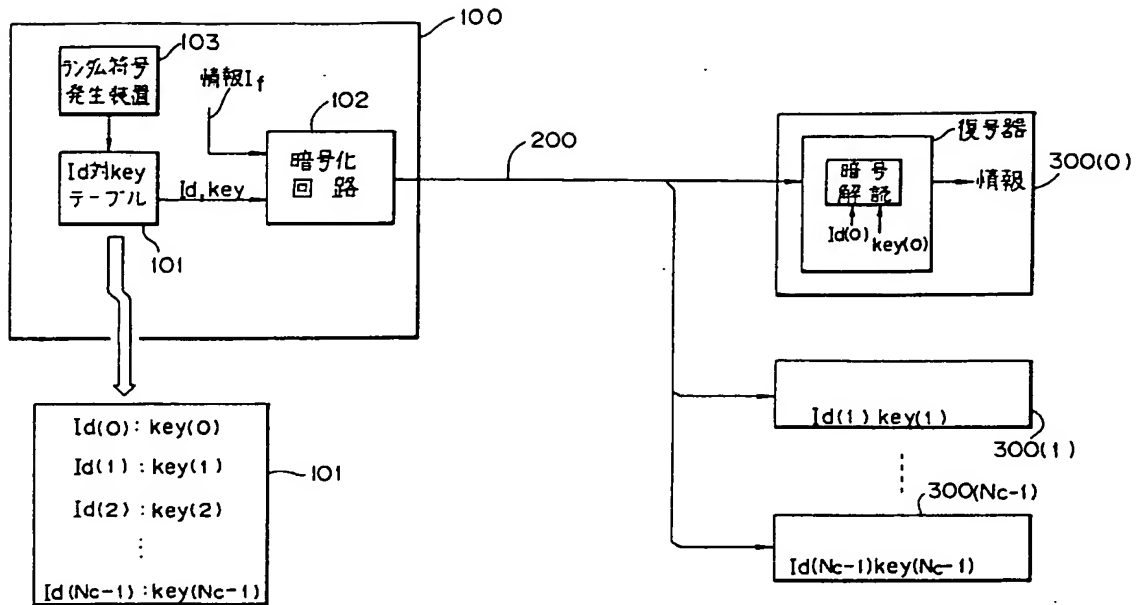
- 周期
n = 124

第12図(2)

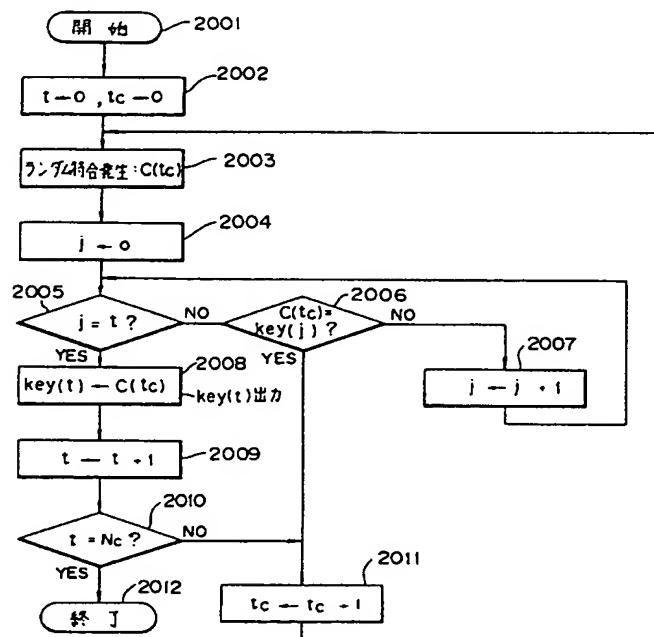
time	Q[]:78543210	Q'[]:7641	code: sa	sb	sc (hex)
00000	10000000	1000	80	40	80
00001	11000000	0100	C0	40	40
00002	01100000	0010	60	50	50
00003	10100000	0110	80	70	30
00004	01010000	0010	50	18	58
00005	00101000	0000	20	28	28
00006	00010100	1110	10	D4	94
00007	00001000	0000	00	08	09
00008	00000100	1111	00	05	07
00009	00000010	0011	00	41	43
00010	00000001	0000	00	13	43
00011	00100000	0000	10	20	20
00012	00100000	1000	10	80	88
00013	00100000	0100	C4	44	44
00014	00100000	0001	31	23	33
00015	00100000	0001	31	23	33
00016	00100000	0001	31	23	33
00017	00100000	0001	31	23	33
00018	00100000	0001	31	23	33
00019	00100000	0001	31	23	33
00020	00100000	0001	31	23	33
00021	00100000	0001	31	23	33
00022	00100000	0001	31	23	33
00023	00100000	0001	31	23	33
00024	00100000	0001	31	23	33
00025	00100000	0001	31	23	33
00026	00100000	0001	31	23	33
00027	00100000	0001	31	23	33
00028	00100000	0001	31	23	33
00029	00100000	0001	31	23	33
00030	00100000	0001	31	23	33
00031	00100000	0001	31	23	33
00032	00100000	0001	31	23	33
00033	00100000	0001	31	23	33
00034	00100000	0001	31	23	33
00035	00100000	0001	31	23	33
00036	00100000	0001	31	23	33
00037	00100000	0001	31	23	33
00038	00100000	0001	31	23	33
00039	00100000	0001	31	23	33
00040	00100000	0001	31	23	33
00041	00100000	0001	31	23	33
00042	00100000	0001	31	23	33
00043	00100000	0001	31	23	33
00044	00100000	0001	31	23	33
00045	00100000	0001	31	23	33
00046	00100000	0001	31	23	33
00047	00100000	0001	31	23	33
00048	00100000	0001	31	23	33
00049	00100000	0001	31	23	33
00050	00100000	0001	31	23	33
00051	00100000	0001	31	23	33
00052	00100000	0001	31	23	33
00053	00100000	0001	31	23	33
00054	00100000	0001	31	23	33
00055	00100000	0001	31	23	33
00056	00100000	0001	31	23	33
00057	00100000	0001	31	23	33
00058	00100000	0001	31	23	33
00059	00100000	0001	31	23	33
00060	00100000	0001	31	23	33
00061	00100000	0001	31	23	33
00062	00100000	0001	31	23	33
00063	00100000	0001	31	23	33
00064	00100000	0001	31	23	33
00065	00100000	0001	31	23	33
00066	00100000	0001	31	23	33
00067	00100000	0001	31	23	33
00068	00100000	0001	31	23	33
00069	00100000	0001	31	23	33
00070	00100000	0001	31	23	33
00071	00100000	0001	31	23	33
00072	00100000	0001	31	23	33
00073	00100000	0001	31	23	33
00074	00100000	0001	31	23	33
00075	00100000	0001	31	23	33
00076	00100000	0001	31	23	33
00077	00100000	0001	31	23	33
00078	00100000	0001	31	23	33
00079	00100000	0001	31	23	33
00080	00100000	0001	31	23	33
00081	00100000	0001	31	23	33
00082	00100000	0001	31	23	33
00083	00100000	0001	31	23	33
00084	00100000	0001	31	23	33
00085	00100000	0001	31	23	33
00086	00100000	0001	31	23	33
00087	00100000	0001	31	23	33
00088	00100000	0001	31	23	33
00089	00100000	0001	31	23	33
00090	00100000	0001	31	23	33
00091	00100000	0001	31	23	33
00092	00100000	0001	31	23	33
00093	00100000	0001	31	23	33
00094	00100000	0001	31	23	33
00095	00100000	0001	31	23	33
00096	00100000	0001	31	23	33
00097	00100000	0001	31	23	33
00098	00100000	0001	31	23	33
00099	00100000	0001	31	23	33

第12図(1)

time	Q[1]:7554310	Q[1]:432	code: me (hex)	L(t)	time	code: me (hex)	R(t)
00188	01010100	011	54		00210	DE	
00189	0001010	100	25		00211	F2	
00190	0001010	100	25		00212	78	
00191	11001010	110	CA		00213	78	
00192	11100101	000	75		00214	BF	
00193	01110100	101	89		00215	9	
00194	10111001	101	DC		00216	18	
00195	11011000	101	77		00217	F8	
00196	11111010	100	88		00218	54	
00197	10111011	101	88		00219	77	
00198	11011011	101	88		00220	77	
00199	11011011	101	88		00221	77	
00200	11011011	101	88		00222	77	
00201	11011011	101	88		00223	77	
00202	11011011	101	88		00224	77	
00203	11011011	101	88		00225	77	
00204	11011011	101	88		00226	77	
00205	11011011	101	88		00227	77	
00206	11011011	101	88		00228	77	
00207	11011011	101	88		00229	77	
00208	11011011	101	88		00230	77	
00209	11011011	101	88		00231	77	
00210	11011011	101	88		00232	77	
00211	11011011	101	88		00233	77	
00212	11011011	101	88		00234	77	
00213	11011011	101	88		00235	77	
00214	11011011	101	88		00236	77	
00215	11011011	101	88		00237	77	
00216	11011011	101	88		00238	77	
00217	11011011	101	88		00239	77	
00218	11011011	101	88		00240	77	
00219	11011011	101	88		00241	77	
00220	11011011	101	88		00242	77	
00221	11011011	101	88		00243	77	
00222	11011011	101	88		00244	77	
00223	11011011	101	88		00245	77	
00224	11011011	101	88		00246	77	
00225	11011011	101	88		00247	77	
00226	11011011	101	88		00248	77	
00227	11011011	101	88		00249	77	
00228	11011011	101	88		00250	77	
00229	11011011	101	88		00251	77	
00230	11011011	101	88		00252	77	
00231	11011011	101	88		00253	77	
00232	11011011	101	88		00254	77	
00233	11011011	101	88		00255	77	
00234	11011011	101	88		00256	77	
00235	11011011	101	88		00257	77	
00236	11011011	101	88		00258	77	
00237	11011011	101	88		00259	77	
00238	11011011	101	88		00260	77	
00239	11011011	101	88		00261	77	
00240	11011011	101	88		00262	77	
00241	11011011	101	88		00263	77	
00242	11011011	101	88		00264	77	
00243	11011011	101	88		00265	77	
00244	11011011	101	88		00266	77	
00245	11011011	101	88		00267	77	
00246	11011011	101	88		00268	77	
00247	11011011	101	88		00269	77	
00248	11011011	101	88		00270	77	
00249	11011011	101	88		00271	77	
00250	11011011	101	88		00272	77	
00251	11011011	101	88		00273	77	
00252	11011011	101	88		00274	77	
00253	11011011	101	88		00275	77	
00254	11011011	101	88		00276	77	
00255	11011011	101	88		00277	77	
00256	11011011	101	88		00278	77	
00257	11011011	101	88		00279	77	
00258	11011011	101	88		00280	77	
00259	11011011	101	88		00281	77	
00260	11011011	101	88		00282	77	
00261	11011011	101	88		00283	77	
00262	11011011	101	88		00284	77	
00263	11011011	101	88		00285	77	
00264	11011011	101	88		00286	77	
00265	11011011	101	88		00287	77	
00266	11011011	101	88		00288	77	
00267	11011011	101	88		00289	77	
00268	11011011	101	88		00290	77	
00269	11011011	101	88		00291	77	
00270	11011011	101	88		00292	77	
00271	11011011	101	88		00293	77	
00272	11011011	101	88		00294	77	
00273	11011011	101	88		00295	77	
00274	11011011	101	88		00296	77	
00275	11011011	101	88		00297	77	
00276	11011011	101	88		00298	77	
00277	11011011	101	88		00299	77	
00278	11011011	101	88		00300	77	
00279	11011011	101	88		00301	77	
00280	11011011	101	88		00302	77	
00281	11011011	101	88		00303	77	
00282	11011011	101	88		00304	77	
00283	11011011	101	88		00305	77	
00284	11011011	101	88		00306	77	
00285	11011011	101	88		00307	77	
00286	11011011	101	88		00308	77	
00287	11011011	101	88		00309	77	
00288	11011011	101	88		00310	77	
00289	11011011	101	88		00311	77	
00290	11011011	101	88		00312	77	
00291	11011011	101	88		00313	77	
00292	11011011	101	88		00314	77	
00293	11011011	101	88		00315	77	
00294	11011011	101	88		00316	77	
00295	11011011	101	88		00317	77	
00296	11011011	101	88		00318	77	
00297	11011011	101	88		00319	77	
00298	11011011	101	88		00320	77	
00299	11011011	101	88		00321	77	
00300	11011011	101	88		00322	77	
00301	11011011	101	88		00323	77	
00302	11011011	101	88		00324	77	
00303	11011011	101	88		00325	77	
00304	11011011	101	88		00326	77	
00305	11011011	101	88		00327	77	
00306	11011011	101	88		00328	77	
00307	11011011	101	88		00329	77	
00308	11011011	101	88		00330	77	
00309	11011011	101	88		00331	77	
00310	11011011	101	88		00332	77	
00311	11011011	101	88		00333	77	
00312	11011011	101	88		00334	77	
00313	11011011	101	88		00335	77	
00314	11011011	101	88		00336	77	
00315	11011011	101	88		00337	77	
00316	11011011	101	88		00338	77	
00317	11011011	101	88		00339	77	
00318	11011011	101	88		00340	77	
00319	11011011	101	88		00341	77	
00320	11011011	101	88		00342	77	
00321	11011011	101	88		00343	77	
00322	11011011	101	88		00344	77	
00323	11011011	101	88		00345	77	
00324	11011011	101	88		00346	77	
00325	11011011	101	88		00347	77	
00326	11011011	101	88		00348	77	
00327	11011011	101	88		00349	77	
00328	11011011	101	88		00350	77	
00329	11011011	101	88		00351	77	
00330	11011011	101	88		00352	77	
00331	11011011	101	88		00353	77	
00332	11011011	101	88		00354	77	
00333	11011011	101	88		00355	77	
00334	11011011	101	88		00356	77	
00335	11011011	101	88		00357	77	
00336	11011011	101	88		00358	77	
00337	11011011	101	88		00359	77	
00338	11011011	101	88		00360	77	
00339	11011011	101	88		00361	77	
00340	11011011	101	88		00362	77	
00341	11011011	101	88		00363	77	
00342	11011011	101	88		00364	77	
00343	11011011	101	88		00365	77	
00344	11011011	101	88		00366	77	
00345	11011011	101	88		00367	77	
00346	11011011	101	88		00368	77	
00347	11011011	101	88		00369	77	
00348	11011011	101	88		00370	77	
00349	11011011	101	88		00371	77	
00350	11011011	101	88		00372	77	
00351	11011011	101	88		00373	77	
00352	11011011	101	88		00374	77	
00353	11011011	101	88		00375	77	
00354	11011011	101	88		00376	77	
00355	11011011	101	88		00377	77	
00356	11011011	101	88		00378	77	
00357	11011011	101	88		00379	77	
00358	11011011	101	88		00380	77	
00359	11011011	101	88		00381	77	
00360	11011011	101	88		00382	77	
00361	11011011	101	88		00383	77	
00362	11011011	101	88		00384	77	
00363	11011011	101	88		00385	77	
00364	11011011	101	88		00386	77	
00365	11011011	101	88		00387	77	
00366	11011011	101	88		00388	77	
00367	11011011	101	88		00389	77	



第17図



第18図